Spring 2020

IT Security Policy Compliance: A University Perspective

Jack D. Barnes
University of New Hampshire, Durham

IT Security Policy Compliance: A University Perspective

Prepared by: Jack Barnes

Advised by: Professor Kholekile Gwebu

Spring 2020

Table of Contents

Introduction:

Security and privacy concerns continue to grow in this constantly evolving, technology-driven world. However, security and privacy policies are rarely fully understood and adhered to. This study investigates university students' awareness of these policies as well as their intentions regarding compliance. Understanding the students' intentions, shaped by beliefs and attitudes, can be used to improve how these policies are written and shared. Understanding if and how students adhere to security and privacy policies may reveal shortcomings in how they are written and shared. Communicating the significance of these policies may improve compliance, ultimately reducing the number of security and privacy concerns.

The main research question this study seeks to investigate is: do warnings about the existence of security policies and the consequences of violating such policies deter noncompliance behavior at university campuses? In many cases, students tend to be unaware of the existence of certain security policies. Moreover, most policies are not explained in detail. They outline the policy in a very general manner and the consequences (often punishment) of noncompliance, but they seldom mention why they are important. One prediction of this study is that if both what the policy is and the reason for its existence are provided to students, there will be an increase in compliance.

The remainder of this thesis is organized as follows. The next section reviews the extant literature on security policy compliance. Next, hypotheses are developed. Thereafter, the methodology used to assess the hypotheses is presented. This is followed by a presentation of the findings and discussion about the implications of the findings for universities. The thesis concludes by pointing out some limitations and avenues for future research.

Literature Review:

There are many factors that influence security policy compliance. The literature in Table 1 below describes factors like attitudes, neutralization, subjective norm, training, punishment expectancy, and reward expectancy. For example, neutralization is an important factor that has been determined to drive information security policy (ISP) compliance (Siponen & Vance, 2010). Neutralization allows employees to fail to comply with ISPs but allows them to think they are not doing anything wrong. Punishment is another important factor that influences compliance with ISPs. Punishment may be necessary for some situations due to the principal-agent relationship between employer and employee. The principal and agent have different goals, and each tries to maximize its own interests. Perceived justice of punishment is a strong determinant of IT compliance (Xue et al., 2011). Another factor is training. Providing additional training is the most common approach to dealing with security and privacy policy noncompliance (Puhakainen & Siponen, 2010) as it increases awareness of security policies. Table 1 summarizes the studies which are most relevant to the current study.

Table 1: Summary of Related Studies

Title	Author	Summary/Findings	Other Concepts / Key Terms:	Limitations
Campus Emergency Notification Systems: An Examination of Factors Affecting Compliance with Alerts	Han, W., Ada, S., Sharman, R., & Rao, H. R. (2015)	Immediate compliance from students regarding campus-wide alerts is vital to improving campus safety. The study's dependent variable is compliance intention. 99% of students complied, some complied immediately, and others verified first. Administered survey with scenarios to test hypotheses: perceived subjective norms, safety threats, and financial threats positively affected compliance. Subjective norm and information quality trust	Subjective norm: perceived social and peer pressures to perform or not perform certain behavior. Common Method Bias	Conducted in the Northern United States. This study focuses on one specific type of compliance: compliance with campus alerts. It does not expand on IS policies.

		are critical factors. Financial threats were not.		
The role of self-control in information security violations: Insights from a cognitive neuroscience perspective	Hu, Q., West, R., & Smarandescu, L. (2015)	This study takes a very scientific look at how one's self-control affects compliance with IS policies. Undergraduates with low self-control were significantly associated with software piracy. In addition, low self-control was the strongest contributor to the intention, primarily through affecting employees' perception of intrinsic and extrinsic benefits of the violations. Main hypothesis: Individuals with low self-control tend to choose actions with near-term gain but potential long-term loss.	Self-control: an individual's ability to refrain from committing deviant or criminal acts under given circumstances	Participants of the study consisted of undergraduate students attending a large public university in the Midwest. The study does not expand on other factors effective compliance, such as neutralization techniques. The study does not explore the importance of how to present the information to students to increase compliance.
Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance	Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019)	Analyzes the current research on the antecedents of security policy compliance to determine the relative importance. Perceived usefulness, personal norms and ethics, attitude, normative beliefs, and organizational support all had a significant effect on compliance intentions (effect size magnitude). Resource vulnerability and rewards did not.	Social and moral influences Rewards Self-efficacy	Data from respondents from countries in Asia-Pacific, Europe, and North America. Only data from full-time employees. Does not explore how organizations can better train and educate employees to enhance their perceived usefulness of security policies. How does the way the policy is presented affect compliance?
Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance	Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018)	This study extends prior neutralization research by adapting three approaches (informational influence, normative influence, and antineutralization communication) into a conceptual model to reduce the intention of employees to violate security policies.	Informational influence: individual behavior is influenced by relevant information, such as the outcomes of the behavior, separate from any sanctions	Participants were full-time U.S employees (mean age of 45.4) Focuses on how simple, short communication can influence behavior. Measured compliance intentions directly

		This study shows that the way organizations communicate security policies can increase compliance. It shows that reinforcing the need for secure behavior through short communications, including even brief informational statements that highlight the reasons why information security policies exist.	Normative influence: individuals conform to the norms of others to preserve a favorable self-presentation Antineutralization communication directly addresses the temptation to neutralize Social desirability bias	after delivering information security communication to the participants. Is there a way to neutralize this factor?
Punishment, justice, and compliance in mandatory IT settings.	Xue, Y., Liang, H., & Wu, L. (2011)	This study examines the necessity of punishment. Punishment is necessary due to the principal-agent relationship between employer and employee. The principal and agent have incongruent goals, and each tries to maximize its own interests. Punishment influences the punished person and other organizational members who observed the punishment event. This study finds that perceived justice of punishment is a strong determinant of IT compliance intention in mandatory settings.	Punishment expectancy Actual punishment Perceived justice of punishment	This research has a glaring limitation. For punishment to alleviate non-compliance issues, the user has to violate a policy first. Very often, punishments are ambiguous to employees, so they neutralize them. In order to feel the impact of punishment (for both the user and other organizational members who observe the punishment), the misconduct must occur first. Participants were from one of China's top 500 enterprises. Chinese business culture is vastly different from the United States.
Organizations' information security policy compliance: Stick or carrot approach?	Chen, Y., Ramamurthy, K., & Wen, K. W. (2012)	Findings highlight that reward enforcement, a remunerative control mechanism in the information systems security context, could be an alternative for organizations where sanctions do not successfully prevent a violation.	Compliance theory General deterrence theory Coercive, remunerative, and normative control: Certainty of control: certainty of	Web-based experiment involving real-world employees in their natural settings with a median age of 35, and the average participant had been at their organization for 7 years.

		Organizations enforce compliance by issuing three types of control: coercive, remunerative, and normative. In coercive control, organizations use threats and punishments ("the stick"). Remunerative control refers to a policy instrument by which organizations use some forms of economic incentives ("the carrot"), such as bonuses, promotions, and commissions. When it comes to normative control, symbolic and moral reasoning are emphasized. The study found that the main effects of severity of punishment, significance of reward, and certainty of control were all significant.	punishment or reward increases compliance	The article does not explore potential benefits from presenting security policies in different ways.
Using accountability to reduce access policy violations in information systems	Vance, A., Lowry, P. B., & Eggett, D. (2013)	The dependent variable in this study is access to policy violations. Designing user-interface elements such that they increase perceived accountability in end-users will ultimately reduce the amount of IS policy violations.	Accountability theory Social presence Group- polarization	Factorial survey: the primary sample consisted of 96 IS majors in two sections of a course on IS business processes and internal control. The subjects were familiar with the topic of IS security policies, access control, and computer abuse. This study had a few limitations. It is one of the most like the research in this study, which involves how the way the policy is presented affects compliance. This study begins to prove explaining why the policy exists increases compliance. Vance's study did something similar; they proved increasing accountability increases compliance.

Understanding nonmalicious security violations in the workplace: A composite behavior model	Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011)	This study highlights the importance of job performance goals and security risk perceptions on shaping user attitudes. It demonstrates the effect of workgroup norms on both user attitudes and behavioral intentions. This study also informs security management practices on the importance of linking security and business objectives.	Perceived security risk	A survey of computer end-users in the workplace consisting of 306 employees. The study examines why many end-users may not comply with IS policies, but it does not explore how to improve compliance.
Understanding employee responses to stressful information security requirements: A coping perspective	D'Arcy, J., Herath, T., & Shoss, M. K. (2014)	This article uses coping theory to explore an underlying relationship between employee stress caused by burdensome, complex, and ambiguous information security requirements and deliberate information security policy violations. The study found that when employees perceive stress due to security requirements, they are more likely to rationalize ISP violations through moral disengagement.	Coping theory	Survey of 539 employees. The findings point to potential mechanisms to reduce the stress of employees. The main ones are precise and clearly written (i.e., devoid of excessive technical jargon and legal terms) security policies. However, the findings do not explain the potential benefit of explaining why a security policy exists.
What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors	Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015)	The fear appeals appear to have had a significant influence on perceived fear, intentions to back up data, and actual data backups performed.	Protection motivation theory	Participants consisted of an undergraduate pool of psychology students at a large university in the United States. Using fear appeals is somewhat similar to this study. The fear appeals are a type of explanation describing why a security policy is in place. However, there is much more research to be done concerning how to present these security policies to students.
Information security policy compliance: an	Bulgurcu, B., Cavusoglu, H.,	This study explains that along with normative belief and self-	Self-efficacy	At the beginning of the survey, each

empirical study of rationality-based beliefs and information security awareness	& Benbasat, I. (2010)	efficacy, an employee's attitude toward compliance determines intention to comply with IS policies. An employee's attitude is influenced by benefit of compliance, cost of compliance, and cost of noncompliance. These beliefs are shaped by the employee's outcome beliefs concerning the events that follow compliance or noncompliance. The results show that an employee's intention to comply with an IS policy is significantly influenced by attitude, normative beliefs, and self-efficacy to comply.	Outcome beliefs Rational choice theory Theory of planned behavior	respondent was asked whether his organization had established an ISP and whether the respondent was aware of the ISP's requirements, and they excluded from the survey those who worked in an organization without a written ISP or who were not aware of the requirements of their organizations' ISPs. The data was collected from full-time employees and does not explain how to present IS policies to positively affect compliance.
Fear appeals and information security behaviors: an empirical study	Johnston, A. C., & Warkentin, M. (2010)	This study analyzes the influence of fear appeals on the compliance of end-users with recommendations to enact specific individual computer security actions toward the mitigation of threats. The results find that both response efficacy and self-efficacy appear to have strong predictive ability, and social influence has an even stronger effect on behavioral intent.	Self-efficacy Response efficacy Threat severity Social influence	Most of the subjects were between the ages of 18 and 29. The study provides very high-level recommendations to increase compliance. For example, one recommendation is as follows: "...security managers may wish to reevaluate their IT security governance strategy to ensure the greatest level of user compliance with organizational security policy" (Johnston and Warkentin 2010). However, there is much more to explore in terms of recommendations.

Ensuring employees' IT compliance: Carrot or stick?	Liang, H., Xue, Y., & Wu, L. (2013)	The intention of this study is to explore how different incentives influence employee compliance. In this case, the incentives are rewards (carrot) and punishments (stick). Results: False: Reward expectancy positively affects IT compliance behavior. True: Punishment expectancy positively affects IT compliance behavior. True: Promotion focus positively moderates the relationship between reward expectancy and IT compliance behavior. True: Prevention focus positively moderates the relationship between punishment expectancy and IT compliance behavior.		All respondents are accountants from a Chinese organization. China's culture is very unique and likely not applicable to Western nations.
Information security policy noncompliance: An integrative social influence model	Gwebu, K., Wang, J., & Hu, M. (2016)	This study addresses the common assumption that desirable beliefs (compliance is beneficial, and noncompliance is damaging) motivate compliance to security and privacy policies, while undesirable beliefs (noncompliance is beneficial, and compliance is damaging) motivate noncompliance to security and privacy policies. The results found that neutralization strongly impacts IS noncompliance. In addition, neutralization "strengthens the efficacy of perceived cost of compliance in motivating noncompliance and weakens the efficacy of perceived cost of noncompliance in inhibiting noncompliance" (Gwebu, Wang, and Hu 2016).	Social desirability bias Common method bias Nonresponse bias	The subject of the study is limited to employees. The survey data was collected through a professional market research firm, so the population is a diverse panel of employees working in different organizations nationwide with no mention of students. The results do not explorer how to mitigate the use of neutralization techniques.

Toward a Unified Model of Information Security Policy Compliance	Moody, G. D., Siponen, M., & Pahnila, S. (2018)	This source reviews 11 current information security behavior models, and proposes a unified model, called the unified model of information security policy compliance (UMISPC).	Theory of reasoned action Health belief model Theory of planned behavior Theory of interpersonal behavior Protection motivation theory Deterrence theory and rational choice theory Theory of self-regulation Extended parallel processing model Control balance theory	Future research is needed to examine to what extent the UMISPC can explain different types of ISS behaviors. This source does not explore how to write and present IS policies in a way that increases compliance.
Improving Employees' Compliance through Information Systems Security Training: An Action Research Study	Puhakainen, P., & Siponen, M. (2010)	This study expands on the idea that providing additional training is the most common approach to dealing with security and privacy policy noncompliance. The source explains the need for information security training approaches that are based on theories and evaluated empirically.	Universal constructive instructional theory Elaboration likelihood model	The authors used three methods to collect their data (interviews, a survey, and participatory observation), but all of the subjects are full-time employees.
Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations	Siponen, M., & Vance, A. (2010)	The results of the study suggest that neutralization techniques influence employees' intentions to violate information security policies. This provides further incentive for policymakers to take neutralization into account when developing security and privacy policies.		The sample was collected from three Finnish organizations. Not only is this population in a different country with a different culture, the average work experience of each member of the sample is 18 years. The study does not mention students, nor does it mention the significance of

				explaining why a policy exists to limit neutralization.
Beyond Deterrence: An Expanded View of Employee Computer Abuse	Willison, R., & Warkentin, M. (2013)	This source explains how employee noncompliance is typically due to poor training, low employee motivation, weak affective commitment, or individual oversight. These factors are common in the existing literature. But the source also explains how protection motivation, deterrence, planned behavior, self-efficacy, individual adoption factors, organizational commitment, and other individual cognitive factors are also significant. Intentional computer abuse to harm the company is also apparent in many organizations, and policymakers need to take this into account.		The research was done surveying many employees of various organizations with information security concerns but makes no mention of students. The results of this study do point to various changes policymakers can implement to positively affect compliance, but no research is done to determine if these changes will help.
An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric.	Johnston, A. C., Warkentin, M., & Siponen, M. (2015)	This study explains how fear appeals are very often used to increase compliance of privacy and security policies. The authors focus on finding empirical assessments of the effectiveness of fear appeals. They argue the conventional fear appeal rhetorical framework is inadequate, and they propose "an enhanced fear appeal rhetorical framework that leverages sanctioning rhetoric as a secondary vector of threats to the human asset, thereby adding the dimension of personal relevance" (Johnston, Warkentin, and Siponen 2015).		The use of intention as opposed to actual behavior as the dependent variable. The question of progression from intention to actual behavior is a significant limitation. The data was collected from multiple sub organizations within the same city government in Finland. The study does not explore how to limit noncompliance of privacy and security policies.

Table 1 highlights that there are several factors that can influence security policy compliance. Nevertheless, the role of various contingency factors has not been fully explored.

One important contingency factor is the setting under which the policy is administered. Many prior studies have been conducted in a workplace setting. It should be highlighted that one exception in the table above is the work by Hu, West, and Smarandescu (2015), who examine at students' self-control affects compliance to IS policies. An important question in this study is, do the findings from prior studies in the workplace settings transfer to other settings with different types of subjects such as universities? Additionally, in settings such as universities, are there contexts/scenarios under which policy compliance would differ?

Hypothesis Development:

To explore these questions, a study was designed for a university setting. In the study, some students were informed about the existence of a security policy and were presented with it whereas others were not. Additionally, the scenario under which the students were warned/not warned was varied. One scenario involves a common practice on university campuses known as piggybacking. Piggybacking is a violation of security protocols and entails using one's security credentials to permit unauthorized users to enter a building. Because this practice is very common and many students do not see it as having severe personal consequences, it is likely that even with warnings about the implications of violating the security protocols, students are still unlikely to comply. It is therefore hypothesized that:

H1: In a scenario involving piggybacking, there will not be a significant difference in intention to comply between students who receive a warning about the importance of compliance and those who do not.

The second scenario involves sharing one's Wi-Fi credentials to allow unauthorized users to access the university network. While this practice is likely to occur, perhaps it is much less common due the perceived ramifications. Sharing one's credentials can result in personal

loss/consequences such as identity theft and online stalking or harassment. A reminder about the university policy and the ramifications of noncompliance is likely to trigger compliance. It is therefore hypothesized that:

H2: In a scenario involving sharing a Wi-Fi password, there will be a significant difference in intention to comply between students who receive a warning about the importance of compliance and those who do not. Students who receive the warning will have a higher intention to comply than those who do not.

Materials and Procedure:

To test the above hypotheses, an electronic survey was administered to 140 students at the University of New Hampshire. The survey included demographic questions, different scenarios, and questions about those scenarios. The subjects began the study by reviewing a consent form that outlined the purpose of the study, how the data for the study would be stored, and who at the UNH IRB to contact if they had questions about their rights as a research subject. After consenting to participate in the study, the subjects were randomly assigned to one of the four treatment conditions/scenarios. The figures below illustrate each of the scenarios:

Figure 1: Scenario 1: Piggyback Control

Please read the following very carefully:

All residence halls and undergraduate apartment buildings are equipped with an electronic card access system that allows authorized students to gain access to a building by swiping their University ID card through a card reader located at designated exterior doors.
One day as Jeff is approaching his residence hall, he notices Kathy standing outside the door. She approaches him and asks if she can tag along after he opens the door so that she can get her key. She says she forgot it in her room. Jeff agrees and allows her to enter the building after swiping his ID.
Allowing individuals who seek entry to "piggyback" (enter the building without using their own entry card) can compromise the security of other students and is prohibited. Students found responsible of such behaviors are subject to disciplinary action.

Figure 2: Scenario 2: Piggyback Treatment

Please read the following very carefully:

All residence halls and undergraduate apartment buildings are equipped with an electronic card access system that allows authorized students to gain access to a building by swiping their University ID card through a card reader located at designated exterior doors.
One day as Jeff is approaching his residence hall, he notices Kathy standing outside the door. She approaches him and asks if she can tag along after he opens the door so that she can get her key. She says she forgot it in her room. Jeff agrees and allows her to enter the building after swiping his ID.
Allowing individuals who seek entry to "piggyback" (enter the building without using their own entry card) can compromise the security of other students and is prohibited. The Risks of Piggybacking include:

Theft.

Allowing unauthorized individuals into secured areas can result in tangible losses such as loss of:

- Equipment
- Intellectual property
- Sensitive hardware
- Personal items such as phones, wallets, purses and other valuable items

Unsafe Environment.

An unsecured environment that does not have access controls is more susceptible to:

- Violence
- Active shooter
- Acts of terrorism

Students found responsible of such behaviors are subject to disciplinary action

Figure 3: Scenario 3: Wi-Fi Control

Please read the following very carefully:

Members of the university community have access to various IT resources, including the UNH Secure Wireless Network, which provides the peace-of-mind security of a wired network with the mobility of wireless.
One day, Kathy comes to visit campus. Kathy would like to connect to UNH Secure in order to pay back Jeff some money that she borrowed from him. She hands Jeff her phone and asks him to log her onto UNH Secure so that she can transfer the funds using a secure network. Jeff takes her phone and enters his credentials to connect to UNH Secure.

Figure 4: Scenario 4: Wi-Fi Treatment

Please read the following very carefully:

Members of the University community have access to various IT resources, including the UNH Secure Wireless Network, which provides the peace-of-mind security of a wired network with the mobility of wireless.
One day, Kathy comes to visit campus. Kathy would like to connect to UNH Secure in order to pay back Jeff some money that she borrowed from him. She hands Jeff her phone and asks him to log her onto UNH Secure so that she can transfer the funds using a secure network. Jeff takes her phone and enters his credentials to connect to UNH Secure.
UNH has a policy that prohibits students from allowing unauthorized users from accessing the UNH Secure network. Allowing unauthorized individuals to use the university secure network can result in:

Damage and Theft.

- Destruction of university data
- Identity theft
- Sabotage university systems
- Physical damage to connected devices

Unsafe Environment.

- Online stalking or harassment
- Cyberbullying
- Cyberterrorism

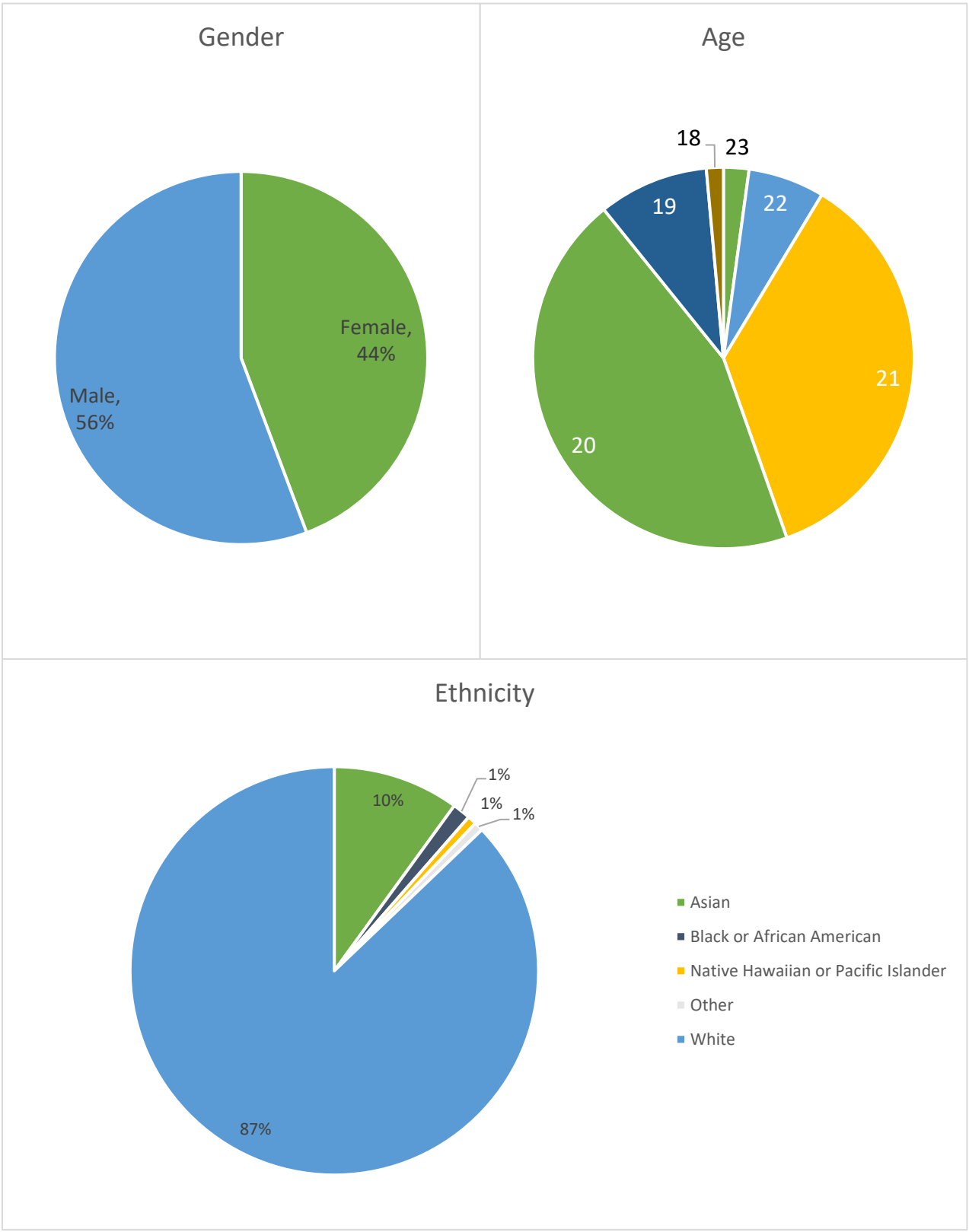
Students found responsible of such behaviors are subject to disciplinary action.

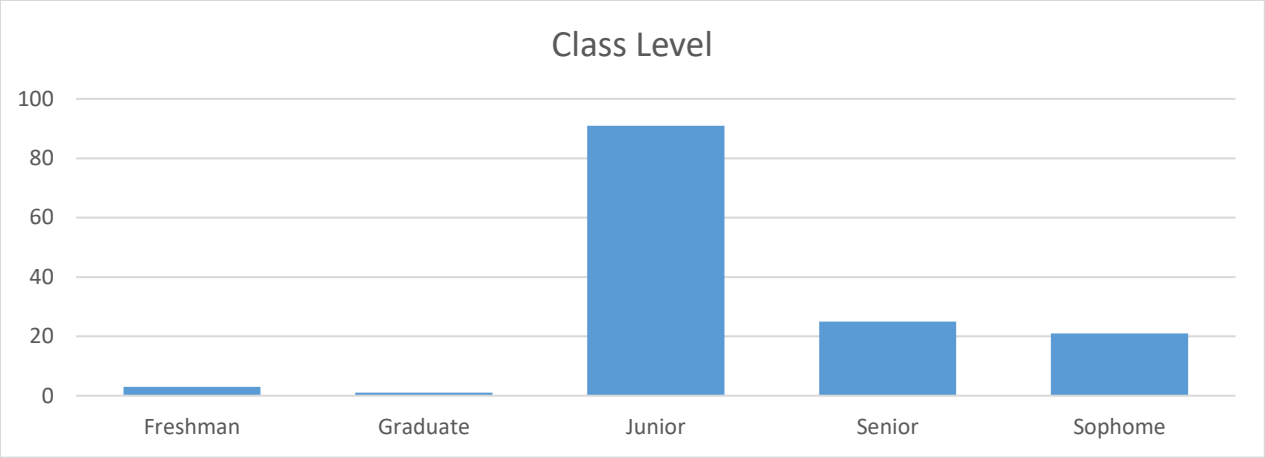
After reading their assigned scenarios the subjects were asked a series of questions. See Appendix 1 for the list of questions. One question (which served as the dependent variable) sought to determine their intention to comply i.e. "I would act in the same way as Jeff did if I were in the same situation." This question was answered on a seven-point scale: Strongly Agree – Strongly Disagree. Other questions focused on the students' Attitude towards the policy, Subjective Norm, Behavioral Control, and Neutralization. Finally, the subjects answered a set of demographic questions to capture their age, race, class level, and major.

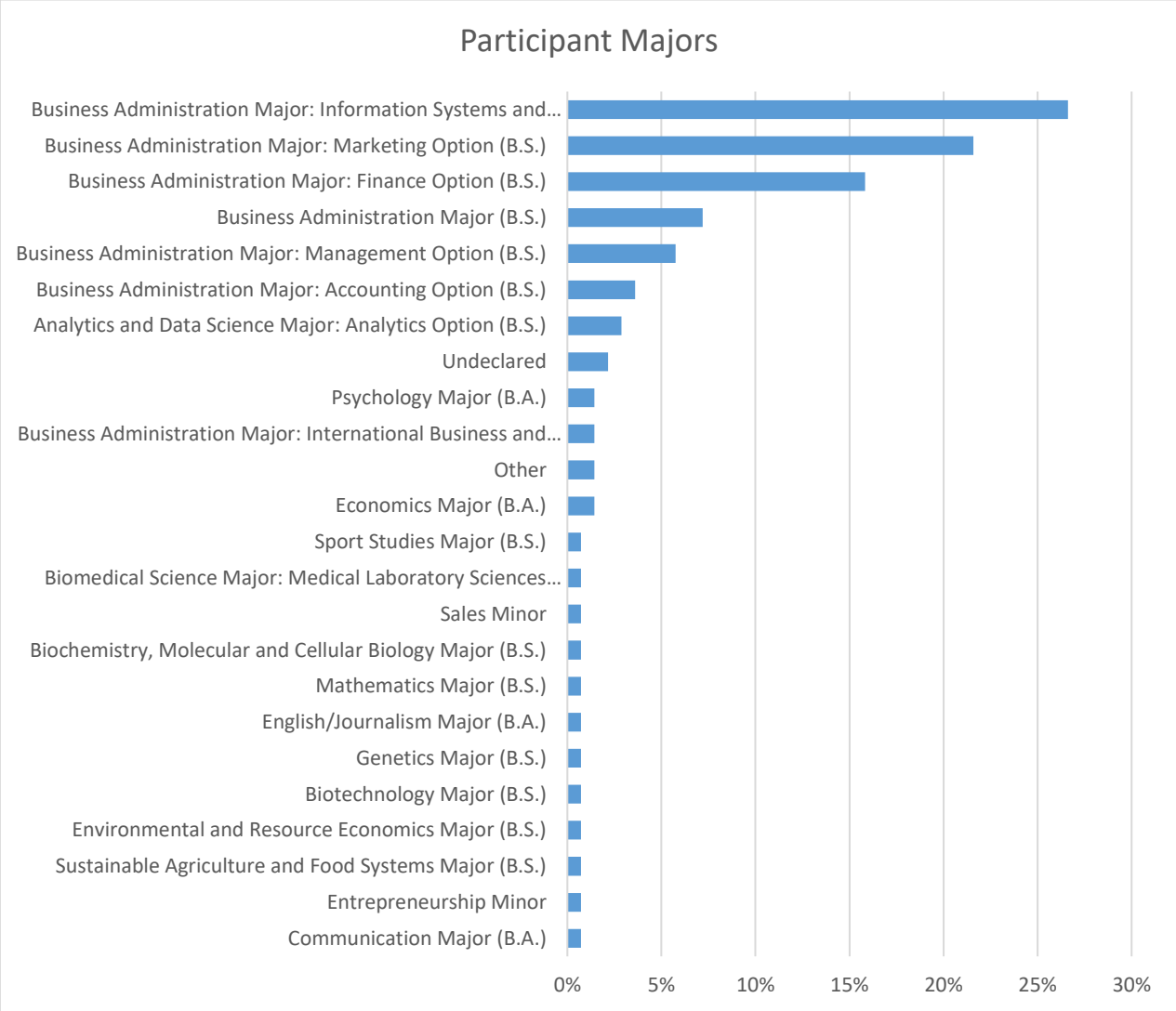
Participants:

The participants in this study consisted of 140 students from the University of New Hampshire. The majority were male (56%). Their ages ranged from 18-23 years (mean = 21 years old). The large majority of respondents were white (87%) with Asian respondents taking up the second largest group (10%). The first seven most common majors were all in the business school, taking up the vast majority of the respondents (83%). The figures below summarize the respondents' profiles.

Figure 5: Participant Demographics




Class Level
100
80
60
40
20
0
Freshman
Graduate
Junior
Senior
Sophome


Participant Majors
Business Administration Major: Information Systems and...
Business Administration Major: Marketing Option (B.S.)
Business Administration Major: Finance Option (B.S.)
Business Administration Major (B.S.)
Business Administration Major: Management Option (B.S.)
Business Administration Major: Accounting Option (B.S.)
Analytics and Data Science Major: Analytics Option (B.S.)
Undeclared
Psychology Major (B.A.)
Business Administration Major: International Business and...
Other
Economics Major (B.A.)
Sport Studies Major (B.S.)
Biomedical Science Major: Medical Laboratory Sciences...
Sales Minor
Biochemistry, Molecular and Cellular Biology Major (B.S.)
Mathematics Major (B.S.)
English/Journalism Major (B.A.)
Genetics Major (B.S.)
Biotechnology Major (B.S.)
Environmental and Resource Economics Major (B.S.)
Sustainable Agriculture and Food Systems Major (B.S.)
Entrepreneurship Minor
Communication Major (B.A.)
0%
5%
10%
15%
20%
25%
30%

Findings:

Figure 6 below shows that respondents who received the piggyback treatment in the form of the additional explanation had virtually no effect on whether they thought they would repeat the subject in the scenario's non-compliant behavior. In fact, no one from the treatment groups said they would be extremely likely, moderately unlikely, or even slightly unlikely they would repeat the subject in the scenario's non-compliant behavior. In other words, most if not all the treatment respondents said they would still likely repeat the subject in the scenario's no-compliant behavior despite the additional explanation of the significance of the policy. This means it would be a waste of time for UNH administration to attempt to warn students to increase compliance to this piggybacking policy. It seems the students will piggyback anyway.

Figure 6: What is the chance you would do what Jeff did in the scenario (Piggybacking)?

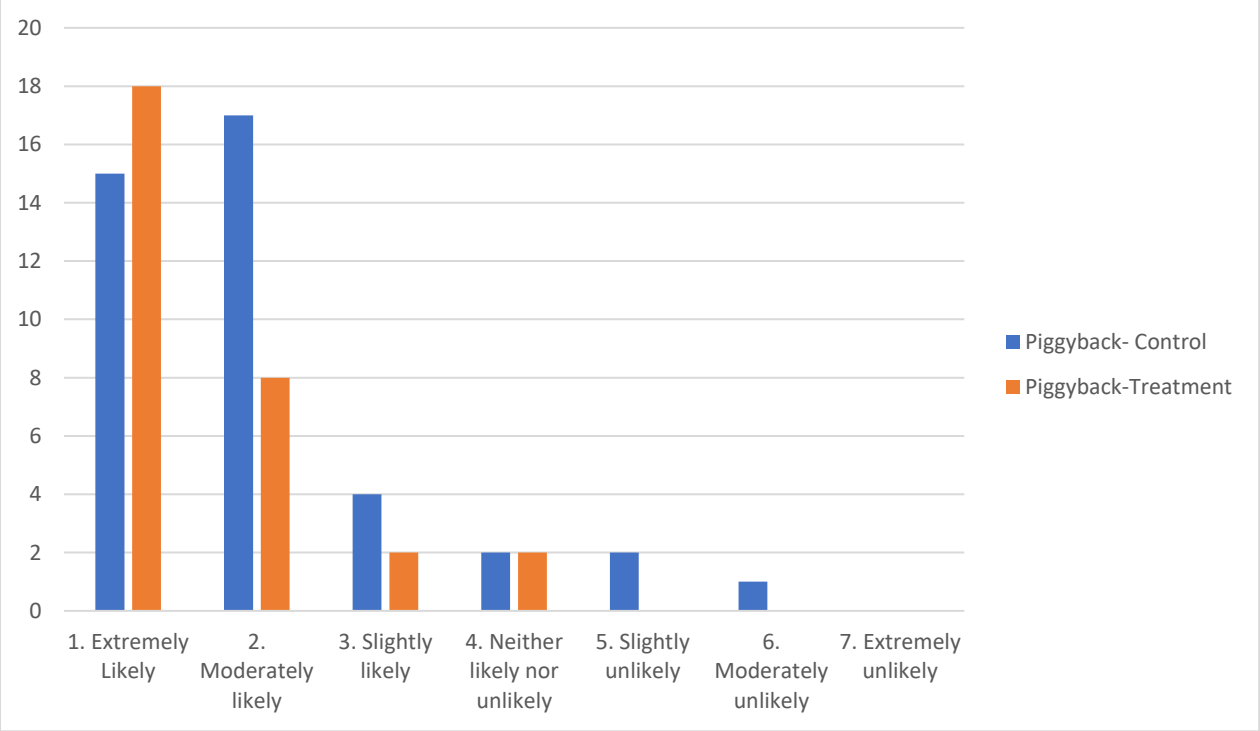
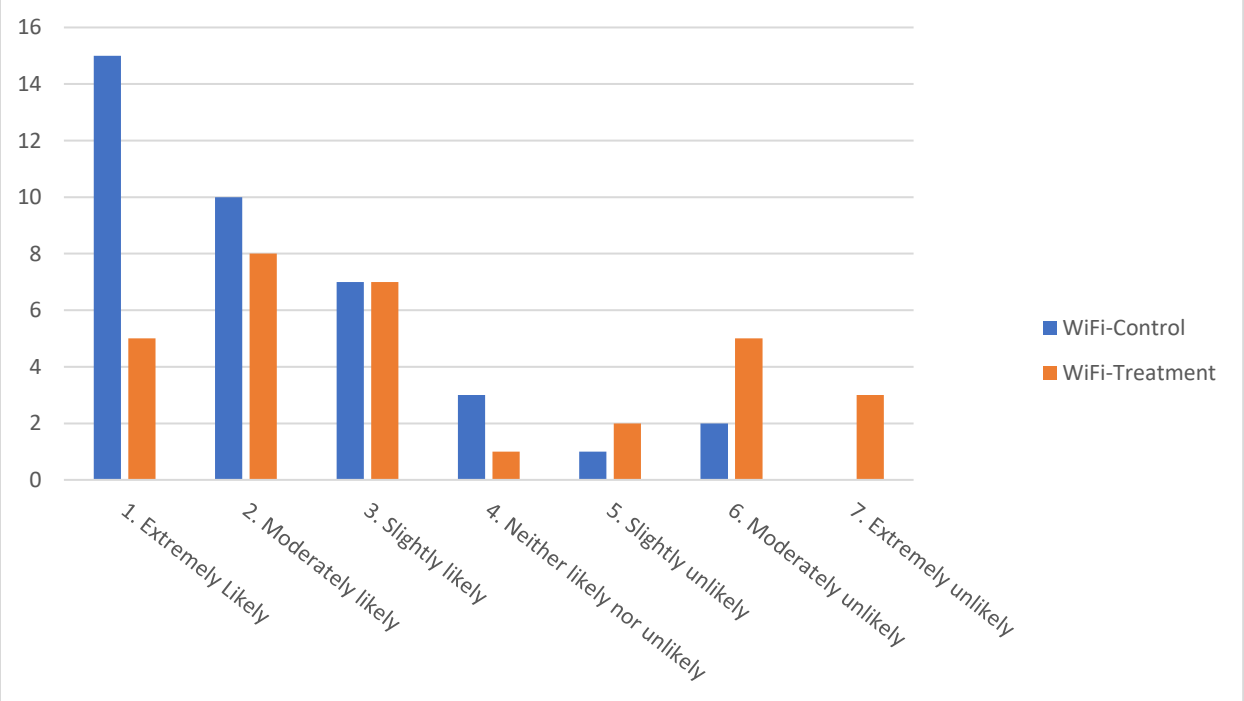


Figure 7 below shows that respondents who received the Wi-Fi treatment in the form of the additional explanation were less likely to repeat the subject in the scenario's non-compliant

behavior. The x-axis is the likelihood, and the y-axis is the number of respondents. The two data points for "1. Extremely Likely" are the most significant. There is a very significant difference between the control and treatment groups. There were fifteen people in the control group who said they would replicate the subject in the scenario's non-compliant behavior, but there were only five people in the treatment group who said they would replicate the subject in the scenario's non-compliant behavior. It is also worth noting that not a single person from the control group said they would be extremely unlikely to repeat the subject in the scenario's non-compliant behavior.

After reading the described scenario in which the subject in the scenario fails to comply with either the piggybacking or Wi-Fi policy at UNH, the respondent was asked what percentage of students they think have repeated the subject in the scenario's non-compliant behavior.

Figure 7: What is the chance you would do what Jeff did in the scenario (Wi-Fi)?



An independent samples t-test is used to statistically compare the mean differences between the treatment and control groups. A p-value less than or equal to 0.05 is considered statistically significant. Table 2 shows the mean values for each scenario under the treatment and control conditions.

Table 2: Dependent Variable: Intention to Not Comply

		N	Mean	Std. Deviation	Std. Error Mean	t	Sig.
Piggyback Treatment	Yes	30	6.4000	0.89443	0.16330	1.785	0.079
	No	41	5.9268	1.23268	0.19251		
Wi-Fi Treatment	Yes	32	4.6250	2.04387	0.36131	-2.750	0.008
	No	38	5.7632	1.40336	0.22765		

Table 2 shows that 30 students received the warning Piggyback treatment (i.e. scenario 2) while 41 students received the control/no warning Piggyback treatment (scenario 1). The findings reveal that the mean for the warning group (M=6.40) was higher than the mean for the no warning group (M=5.93). Nevertheless, this difference in means (0.47) is not statistically significant. This finding is in line with H1 which suggests that in a scenario involving piggybacking there will not be a significant difference in intention to comply between students who receive a warning about the importance of compliance and those who do not.

For the Wi-Fi scenario, 32 students received the warning treatment (i.e. scenario 4), and 38 students received the control/no warning treatment (Scenario 3). The findings in Table 2 show that the mean for the warning group (M=4.63) was lower than the mean for the no warning group (M=5.76). Moreover, this difference in means (1.13) is statistically significant. This finding lends support to H2 that suggests that in a scenario involving sharing a Wi-Fi password subjects who receive a warning will be more likely to comply than those who do not.

To gain insights into the potential sources of differences in the intention to comply, the treatment and control conditions for each of the scenarios are compared across four dimensions (i.e. Attitude, Subjective Norm, Behavioral Control, and Neutralization). The section below summarizes the findings of the comparisons. Subjective norm refers to how someone close to the respondent would feel if that person found out the respondent failed to comply with the policy (Gwebu et al., 2020). Attitude refers to how the respondents felt about the policy itself (Gwebu et al., 2020). Behavioral control refers to the respondents' feeling of control over the situation regarding compliance to the policy (Gwebu et al., 2020). Neutralization refers to the extent to which the respondents minimize the significance of their own non-compliant behavior by attempting to justify it (Gwebu et al., 2020).

Table 3 below shows that the only p-value that was significant for any of the variables was the neutralization p-value (0.023). The rest of the p-values were all above 0.05. Thus, the warning in the Piggyback scenario only had a significant effect on how much students neutralized potential non-compliant behavior but had no effect on their attitude, level of behavioral control, or subjective norm.

Table 3: Piggybacking Scenario Differences in Means

		N	Mean	Std. Deviation	Std. Error Mean	t	Sig
Attitude	Treatment	30	3.5778	1.10358	0.20148	0.320	0.750
	Control	41	3.4878	1.21814	0.19024		
Behavioral Control	Treatment	30	3.8500	1.28083	0.23385	0.029	0.977
	Control	41	3.8415	1.19603	0.18679		
Subjective Norm	Treatment	30	5.6500	1.02470	0.18708	0.915	0.363
	Control	41	5.3841	1.32653	0.20717		
Neutralization	Treatment	30	4.6222	0.85650	0.15637	2.330	0.023
	Control	41	4.0244	1.19812	0.18712		

Table 4 below shows that three out of four of the variables had significant p-values (Attitude: p=0.021, Subjective Norm: p=0.038, Neutralization: p<0.001). So, the treatment scenario had a significant effect on the respondents' attitudes, feelings towards the subjective norm, and extent of neutralization for their potential non-compliant behavior.

Table 4: Wi-Fi Scenario Differences in Means

		N	Mean	Std. Deviation	Std. Error Mean	t	Sig
Attitude	Treatment	32	4.0521	1.13311	0.20031	2.361	0.021
	Control	38	3.3947	1.18259	0.19184		
Behavioral Control	Treatment	32	4.4219	1.17164	0.20712	-0.279	0.781
	Control	38	4.5000	1.16248	0.18858		
Subjective Norm	Treatment	32	4.9609	1.46479	0.25894	-2.118	0.038
	Control	38	5.6776	1.36301	0.22111		
Neutralization	Treatment	32	3.3750	1.36718	0.24169	-4.396	0.000
	Control	38	4.8596	1.44079	0.23373		

These findings suggest those who received the warning had a more negative attitude towards noncompliance, and they felt that the people who are important to them would care if they mimicked the behavior of the character in the scenario. In addition, their ability to justify doing what the character in the scenario did was lower than those who did not receive the warning in this scenario.

Post Hoc Analysis:

Figure 8 shows the percentages of UNH students that each respondent believes have repeated the subject in the scenario's non-compliant behavior for the piggybacking scenario. Both the control group and the piggyback group appear to be similar. There are not many differences between the two groups. This is consistent with Figure 6.

Figure 8: What percentage of students do you think have done what Jeff did (Piggybacking)?

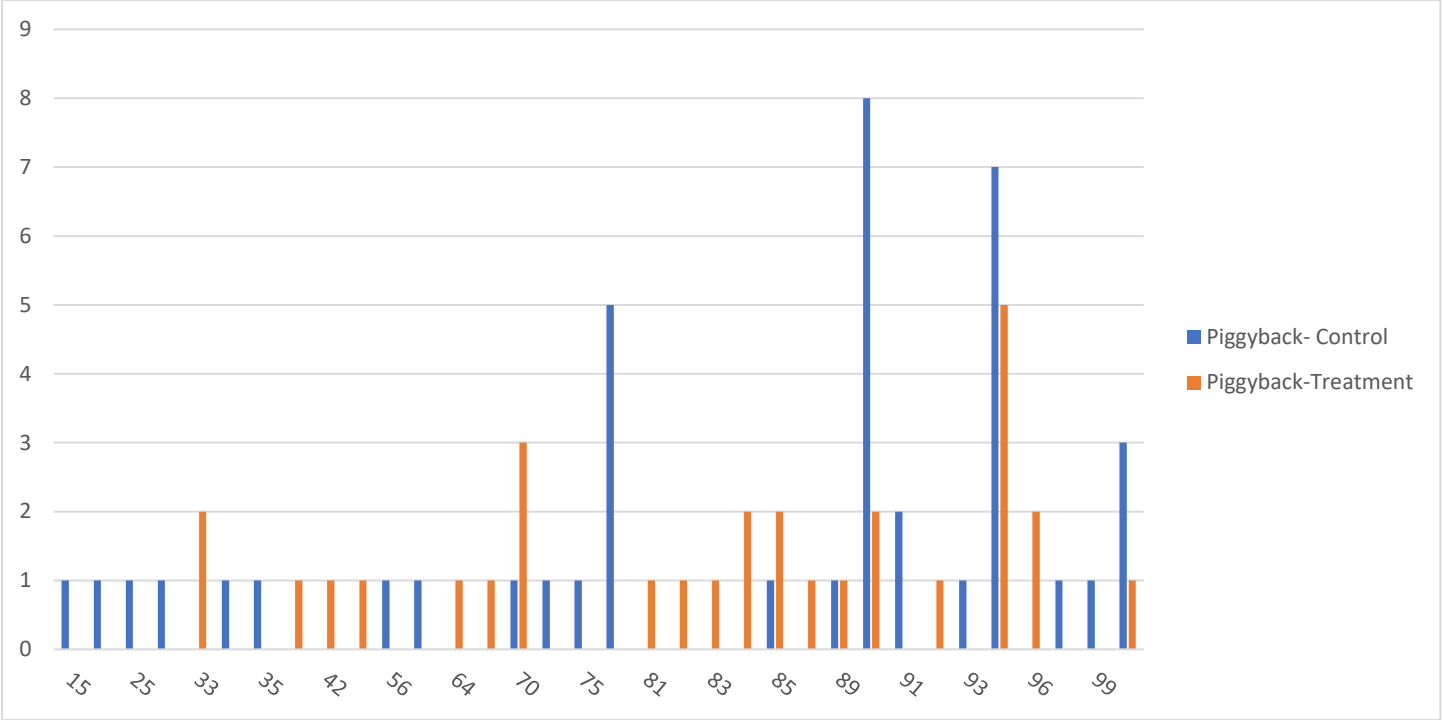
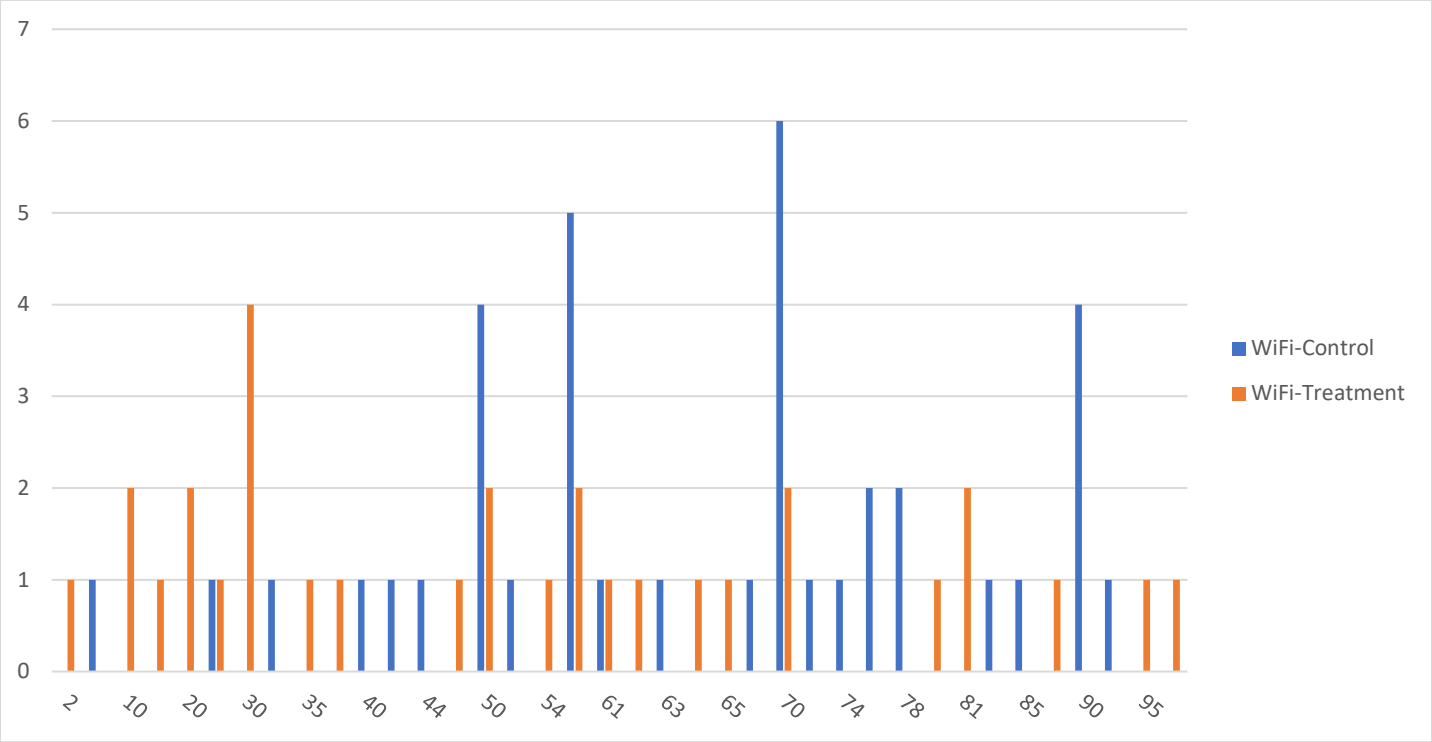


Figure 9 below shows the percentages of UNH students that each respondent believes have repeated the subject in the scenario's non-compliant behavior for the Wi-Fi scenario. Figure 9 above shows the respondents who received the Wi-Fi treatment tend to believe that fewer people would be non-compliant to the policy like the subject in the scenario. The opposite is true as well; the Wi-Fi control group seems to be skewed to the right. More respondents who did not receive the treatment seem to believe that more people would be non-compliant like the subject in the scenario. This is consistent with Figure 7.

Figure 9: What percentage of students do you think have done what Jeff did (Wi-Fi)?



After reading the described scenario in which the subject in the scenario fails to comply with either the piggybacking or Wi-Fi policy at UNH, the respondent was asked if they believe this non-compliant behavior is common practice at UNH. Figure 10 and Figure 11 below show how many of the respondents believe the subject in the scenario's non-compliant behavior is common practice at UNH. Figure 10 shows the piggybacking scenario, and Figure 11 shows the Wi-Fi scenario. Each chart compares the control group who received no warning (shown in blue), and the group who did receive a warning with further explanation about why the policy is important (shown in orange).

Figure 10: What Jeff did is common practice at UNH (Piggybacking)

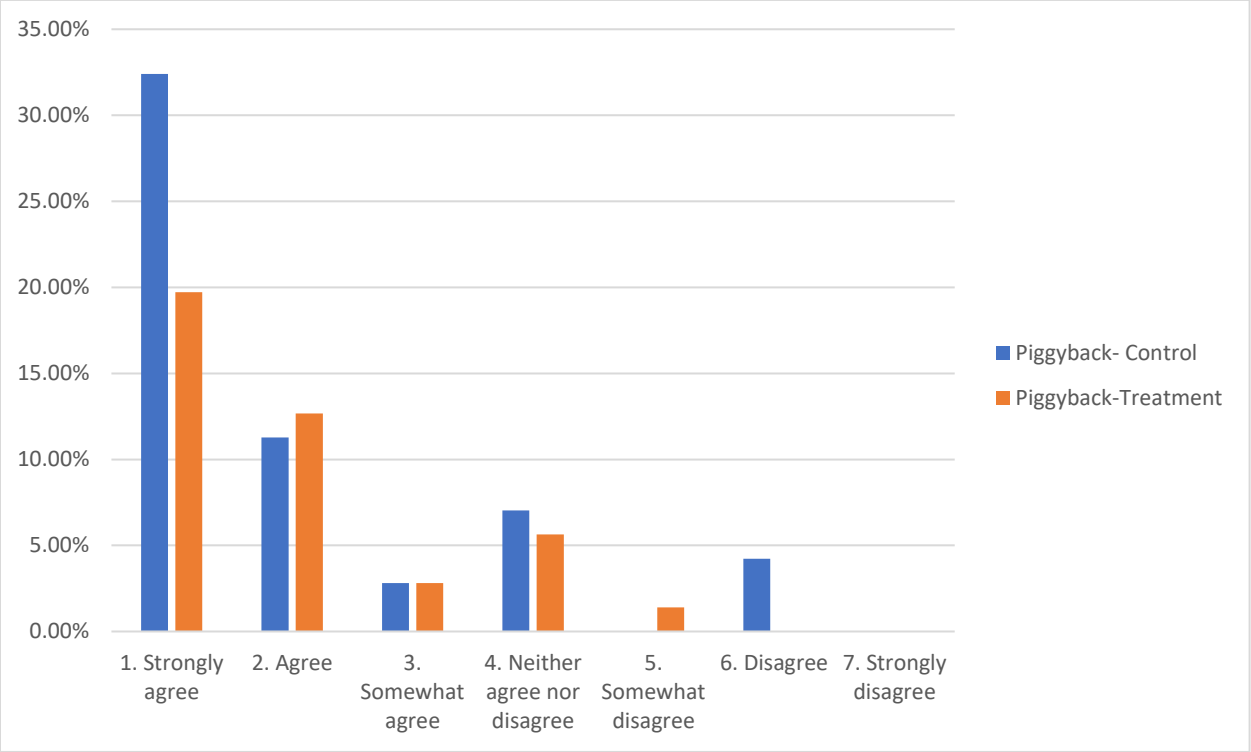


Figure 10 above shows how many of the respondents believe the subject in the scenario's non-compliant behavior is common practice at UNH for the piggybacking scenario. Once again, similar to Figure 6 and Figure 8, Figure 10 does not show a large discrepancy between the control and treatment groups. This has been consistent for each question for respondents who received the piggybacking scenarios. Both the control and treatment groups are skewed to the left. In other words, both groups seem to believe that piggybacking is common practice at UNH.

Figure 11: What Jeff did is common practice at UNH (Wi-Fi)

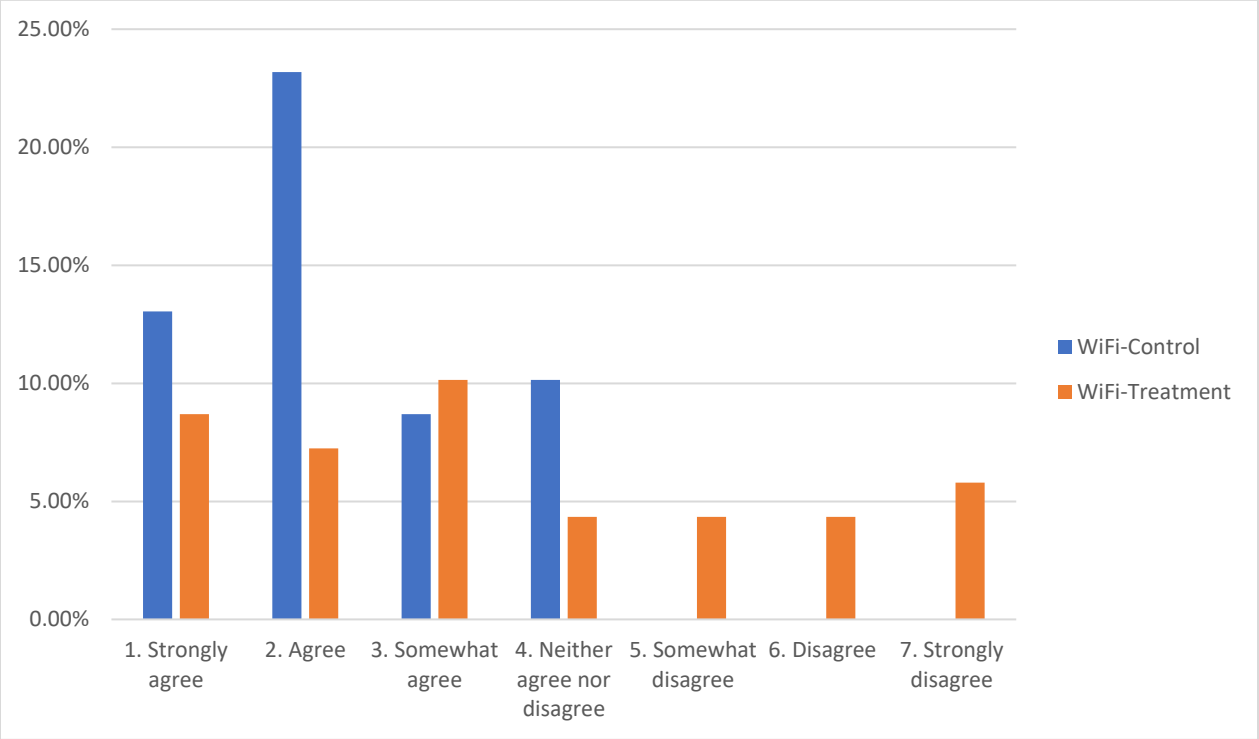


Figure 11 above shows how many of the respondents believe the subject in the scenario's non-compliant behavior is common practice at UNH for the Wi-Fi scenario. This chart shows that respondents who received the Wi-Fi treatment tend to believe that fewer people would be non-compliant to the policy like the subject in the scenario. On the other hand, a much greater percentage of the control group believes the subject in the scenario's non-compliant behavior is common practice. In fact, everyone in the control group agreed to some extent that the subject in the scenario's non-compliance to the Wi-Fi policy is common practice at UNH. No one in the control group disagreed to any extent that what the subject in the scenario did is common practice at UNH. Many of the respondents who received the treatment disagreed that this behavior is common practice at UNH.

Discussion and Implications:

The findings from this study appear to indicate that the current method for presenting security/privacy policies in some contexts (e.g. Wi-Fi scenario) seems to be ineffective. This is particularly true in contexts such as the Wi-Fi scenario where students are not aware if other students are violating this policy. However, for the piggybacking scenario, students believe that "everyone" is violating the policy, or they do not perceive the potential for personal loss. Universities should consider alternate approaches of providing students warnings about the ramifications of violating security policies. For the Wi-Fi scenario, the warning appears to deter students from not complying with the policies. Thus, the UNH administration can expect increased compliance if they were to implement some sort of warning for students.

There are many implications of ineffective security policies. Students and faculty who do not comply are risking the safety of themselves and others. The risks of piggybacking include many different types of theft. Allowing unauthorized individuals into secured areas can result in tangible losses such as the loss of equipment, intellectual property, sensitive hardware, and personal items such as phones, wallets, purses, and other valuable items. Piggybacking also compromises the security of students, resulting in an unsafe environment. An unsafe environment that does not have access controls is more susceptible to acts of violence, active shooters, and acts of terrorism.

Similarly, students who do not comply with the policy against sharing student account credentials for unauthorized individuals to obtain access to the university secure network are also putting themselves and others in potential danger. Allowing unauthorized individuals to use the University secure network can result in the destruction of university data, identity theft, sabotaged university systems, and physical damage to connected devices. In addition, non-

compliance to this policy also creates an unsafe environment for students. Students and faculty are more susceptible to online stalking and harassment, cyberbullying, and cyberterrorism.

It is clear there are many risks resulting from the failure of students to comply with these two policies. Therefore, it is important for universities to ensure their students are aware of these policies and understand why they exist. Explaining the significance of the policy will improve compliance with policies like the Wi-Fi scenario, so universities should find ways to increase student awareness of the importance of these policies. For example, when a student signs into a university's secured network, the university can implement a short warning before signing in explaining the potential risks of unauthorized individuals signing on to this network.

Limitations and Future Research:

This study begins to explain why policymakers need to change the way policies are presented to students. It is clear the current methods are ineffective. However, future research is needed to understand why the differences between the control and treatment groups in the respondents' attitudes towards the policies, subjective norm, and neutralization for non-compliant behavior were significant for the Wi-Fi scenario but not the piggybacking scenario. Perhaps the perceived personal consequences of not holding the door open for someone are far too great compared to the potential risks, or perhaps the policies are just not strictly enforced.

This study focused on two main policies: the policy against piggybacking and the policy against sharing student account credentials so visitors external to UNH can access the Wi-Fi. Further research on additional policies would be helpful to determine why the additional explanation of the Wi-Fi policy changed students' attitudes, but the additional explanation of the piggybacking policy did not change students' attitudes. Analyzing more security and privacy

policies will help us better understand how to best explain policies and spread awareness to students.

Another limitation of this study was the focus of a single university. It is unclear if the findings in this study can be generalized to other universities. There were also limitations with the respondents. The respondents were mostly undergraduate students, so future research on graduate students is needed. The large majority of respondents were white (87%), and the first seven most common majors were all in the business school, taking up the vast majority of the respondents (83%). This means our respondents were not very diverse, so the conclusions may not necessarily be generalizable to campuses with different demographic profiles.

References:

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems*, *19*(8), 689–715. https://doi-org.unh.idm.oclc.org/10.17705/1jais.00506

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523-A7. https://doi-org.unh.idm.oclc.org/10.2307/25750690

Cram, W. A., D, A. J., & Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, *43*(2), 525–554. https://doi-org.unh.idm.oclc.org/10.25300/MISQ/2019/15117

Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information security policy noncompliance: An

integrative social influence model. *Information Systems Journal*, *30*(2), 220–269. https://doi-org.unh.idm.oclc.org/10.1111/isj.12257

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285-A22, http://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=127748832&site=ehost-live

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 767-A4, http://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=54990496&site=ehost-live

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487-A12. https://doi.org/10.2307/25750688

Xue, Y., Liang H., & Wu, L. (2011). Punishment, Justice, and Compliance in Mandatory IT Settings. Information Systems Research, 22(2), 400–414. https://doi-org.unh.idm.oclc.org/10.1287/isre.1090.0266

Appendix 1: Questionnaire

Variable	Question
Intention	What is the chance that you would do what Jeff did in the described scenario?
Neutralization1	If I were to do what Jeff did it would be: - Not Justified:Justified
Neutralization2	If I were to do what Jeff did it would be: - Not a good idea:A good idea
Neutralization3	If I were to do what Jeff did it would be: - Foolish:Wise
SubjectiveNorm1	If I did what Jeff did my : - friends would not care
SubjectiveNorm2	If I did what Jeff did my : - classmates would not care
SubjectiveNorm3	If I did what Jeff did my : - family members would not care
SubjectiveNorm4	If I did what Jeff did my : - my professors would not care
BehaviorControl1	I believe that if I were Jeff - The decision to allow Kathy to do what they did in the scenario is beyond my control
BehaviorControl2	I believe that if I were Jeff - I am confident that I could prevent Kathy from doing what she did.
BehaviorControl4	Please state the extent to which you agree or disagree with the following statements: - Something terrible will happen if I do what Jeff did.
Attitude1	Please state the extent to which you agree or disagree with the following statements: - Though doing what Jeff did is potentially harmful, I am going to be okay.
Attitude2	Please state the extent to which you agree or disagree with the following statements: - I am afraid of what may happen if I do what Jeff did.
Attitude3	Please state the extent to which you agree or disagree with the following statements: - Doing as Jeff did could cause a serious problem.
Observed Frequency of Behavior	What Jeff did is - common practice at UNH
Perceived Occurrence of Behavior	What percentage of students do you think have done what Jeff did? - .
Age	In which year where you born?
Gender	Gender - Selected Choice
Class Level	Class Level-Selected Choice
Major	Major - Selected Choice
Race	What is your ethnicity - Selected Choice